United Nations

Framework Convention on Climate Change

FCCC/SBI/2014/INF.6

Distr.: General
19 May 2014

English only

Subsidiary Body for Implementation
Fortieth session
Bonn, 4–15 June 2014

Item 6(f) of the provisional agenda
Matters relating to the mechanisms under the Kyoto Protocol
Matters relating to the international transaction log under the Kyoto Protocol

Options for, and road map to, information security implementation in the registry system

Note by the administrator of the international transaction log

Summary

Subsequent to preliminary efforts by the Security Working Group, this document specifies options for, and a road map to, further implementation of information security controls in systems supporting emissions trading under the Kyoto Protocol. The Subsidiary Body for Implementation may wish to take note of the information contained in this report and decide on further actions to guide the work of the Security Working Group.

GE.14-03132 (E)

1403132

Please recycle

Contents

		Paragraphs	*Page*
I.	Introduction	1–5	3
	A. Mandate	1–4	3
	B. Possible action by the Subsidiary Body for Implementation	5	3
II.	Information security	6–23	4
	A. Overview	6–8	4
	B. Scope of information security management system	9–13	4
	C. Security Working Group review of threats and vulnerabilities	14–15	5
	D. Security Working Group review of risks and consequences	16–18	6
	E. Security Working Group evaluation of controls	19–23	6
III.	Options identified by Security Working Group	24–32	8
	A. Option 1: business as usual	25–29	8
	B. Option 2: further implementation	30–32	8
IV.	Implementation road map	33–39	9
V.	Monitoring and continuous improvement	40–45	11
Annex			
	Glossary		12

I. Introduction

A. Mandate

1. The Conference of the Parties serving as the meeting of the Parties to the Kyoto Protocol (CMP), by decisions 3/CMP.1 and 13/CMP.1, and the Conference of the Parties, by decision 24/CP.8, requested each Party included in Annex I to the Convention (Annex I Party) to establish and maintain a national registry to ensure the accurate accounting of the issuance, holding, transfer, acquisition, cancellation, retirement and carry-over of Kyoto Protocol units, and requested the secretariat to establish and maintain an international transaction log (ITL) to verify the validity of transactions proposed by national registries. The ITL and national registries are essential for the implementation of the mechanisms under Articles 6, 12 and 17 of the Kyoto Protocol.

2. The CMP, by decision 12/CMP.1, requested the Subsidiary Body for Implementation (SBI) to consider, at its future sessions, the annual reports of the ITL administrator, with a view to requesting the CMP to provide guidance in relation to the operation of national registry systems.

3. The eighth annual report of the ITL administrator[1] provided recommendations to the CMP at its eighth session based on lessons learned during the first commitment period of the Kyoto Protocol. In the recommendations, information security management based on International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001[2] standards were brought to the attention of the CMP. The SBI at its thirty-ninth session requested[3] the ITL administrator and the Security Working Group (SWG) under the Registry System Administrators Forum to further elaborate on options for, and a road map to, information security implementation in national registry systems, for consideration at SBI 40.

4. In order to assess the impact of managing information security based on ISO/IEC 27001 standards, the ITL administrator founded the SWG, which includes representatives of registry system administrators (RSAs) of national registries and the clean development mechanism registry. Following the establishment of objectives and plans to adopt a framework for managing the security of the information assets within the systems supporting emissions trading under the Kyoto Protocol, the SWG identified relevant assets and their associated information security requirements, reviewed known information security threats and selected relevant controls to manage unacceptable risks.

B. Possible action by the Subsidiary Body for Implementation

5. The SBI may wish to take note of the information included in this report and decide on further actions based on the options that the SWG recommends in this document. This will guide the further work of the SWG concerning the implementation of additional information security controls in systems supporting emissions trading under the Kyoto Protocol.

---

[1] FCCC/KP/CMP/2012/8, paragraph 58(b).

[2] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

[3] FCCC/SBI/2013/20, paragraph 83.

II. Information security

A. Overview

6. Information security is focused on the protection of **confidentiality**, **availability** and **integrity** of information. It is achieved by implementing a suitable set of controls, which cover a range of activities related to policies, processes, procedures, organizational structures, software and hardware. These controls need to be selected and implemented in an information security management system (ISMS) to ensure that confidentiality, integrity and availability objectives are met. The selection of controls that effectively treat and manage risks is based upon a risk assessment and risk acceptance levels.

7. Currently, the data exchange standards (DES)[4] mandate a set of security controls that are applied to the interface between the ITL and national registries. A central review of these controls is carried out by the ITL administrator when establishing a registry's readiness to connect to the ITL. Changes in the application of security controls mandated by DES are assessed on an annual basis in the standard independent assessment report (SIAR) process. Further to the mandated controls, additional supplementary controls are applied based on the initiative of national registries.

8. National registries have experienced the consequences of emerging attacks, such as phishing attacks in 2010,[5] and an emergency security procedure has been adopted to address security breaches in national registry systems. The above-mentioned controls mandated in DES or applied by national registry systems, however, do not guarantee consistency in the application of security controls.

B. Scope of information security management system

9. Information assets related to emissions trading under the Kyoto Protocol require adequate protection from unauthorized access and uncontrolled modifications while availability to the emissions trading processes and systems must be assured. The SWG identified information assets consisting of **primary** and **supporting** business processes and information entities based upon guidance from decision 13/CMP.1, DES and SIARs.[6]

10. Primary business processes are processes where loss or degradation makes it impossible to carry out emissions trading under the Kyoto Protocol. These include the unit transaction, reconciliation, administration, data-logging, reporting and account management processes.

11. Primary information is vital for the implementation of the primary business processes. This information consists of strategic data that are partially made available to the public, including the personal information of stakeholders and transaction information representing monetary value. The primary information is related to transactions, registries and accounts.

12. Supporting entities are assets upon which the primary business processes and primary information assets rely. Primarily, these are the supporting information technology (IT) systems that consist of software, hardware and data connections. They also comprise RSAs, developers, site operation staff and authorized account representatives. Finally, they can also include the physical locations that host the primary and supporting assets.

[4] <http://unfccc.int/files/kyoto_protocol/registry_systems/application/pdf/act_des_full_v1.1.10.pdf>.
[5] FCCC/KP/CMP/2010/8.
[6] <http://unfccc.int/kyoto_protocol/registry_systems/independent_assessment_reports/items/4061.php>.

13. Following the identification of the assets, the SWG applied a valuation scale to evaluate the assets based on confidentiality, integrity and availability criteria. All of the assets identified by the SWG have been assessed as **restricted**[7] or **sensitive**.[8] The restricted and sensitive valuations relate to the impact of a degradation, or loss of accuracy, completeness or availability of the assets.

C. Security Working Group review of threats and vulnerabilities

14. Based on the knowledge obtained from recent security incident reviews, the SWG identified known threat sources and assessed the nature of threats as **deliberate**, **accidental** or **environmental**. The threats could originate from special interest groups or internal and environmental sources:

(a) Groups with a special interest in information concerning emissions trading under the Kyoto Protocol that are motivated by potential financial returns, or deliberate disruption or destruction of information. These include organized crime groups, hackers, environmental protection action groups and bodies opposed to increased environmental controls;

(b) Internal sources that consist of RSAs, developers, site operation staff and authorized account representatives. These sources can cause unintentional errors or can have specific interests in abusing existing or obtainable access in order to satisfy their curiosity, commit sabotage or exploit potential financial gains. Internal sources also include external entities who are contracted to operate or maintain the assets or premises holding the assets;

(c) Diverse environmental factors that can influence the assets dispersed on a global scale and can cause physical damage or make services temporarily unavailable.

15. Based on ISO guidance, the SWG identified vulnerabilities related to:

(a) Absent, insufficient or incorrect use of the information security policies, procedures and processes that define the issuance and removal of formal access to assets on predefined levels; the monitoring and reporting of security incidents; the periodic identification and assessment of assets, threats, vulnerabilities and risks, and the allocation of information security roles and responsibilities;

(b) Limited security awareness of internal and third-party resources that operate or maintain emissions trading assets or premises holding these assets. This awareness could be improved by participation in security training, the application of security policies and procedures, meeting formal prerequisites during recruitment and accepting non-disclosure agreements in employment contracts;

(c) Absent, insufficient or incorrect use of:

(i) **Technical** controls that ensure: logging and audit trails, correct system parameters, data encryption, and adequate user identification and authentication mechanisms;

[7] Restricted: if disclosure of the information in scope is not controlled, it can result in major financial loss or damage to public perception. Degradation of its accuracy and completeness or interrupted availability drastically impacts emissions trading under the Kyoto Protocol and is unacceptable.

[8] Sensitive: if the information is leaked outside the organization, it can result in minor financial loss or embarrassment. Degradation of its accuracy and completeness or interrupted availability substantially impacts emissions trading under the Kyoto Protocol and must be avoided.

(ii) **Physical** controls that ensure physical protection and safeguarding from environmental factors;

(iii) **Administrative** controls that ensure: correct installation; regular and planned maintenance; periodic replacement; managed disposal; complete and accessible user and system documentation, and effective change, release and capacity management mechanisms.

D. Security Working Group review of risks and consequences

16. The SWG assessed the impact that might result from the interruption or loss of **confidentiality**, **integrity** or **availability** of the assets supporting emissions trading under the Kyoto Protocol and identified risks originating from the following sources:

(a) Internal or external sources that can impair logical access to emissions trading systems and result in the retrieval, modification or disclosure of sensitive or restricted data used to complete fraudulent transactions;

(b) Internal or external sources that can impair the emissions trading IT systems through inserting covert modifications or malicious code;

(c) Events such as flooding, earthquakes or fire that can limit or cease the ability of sites to support the emissions trading IT systems and resources and prevent their ability to be operated in a safe and reliable way.

17. The SWG conducted an initial risk review and identified the following consequences of emerging threats:

(a) Direct or indirect financial loss due to theft of Kyoto Protocol units or unforeseen costs related to executing emergency procedures;

(b) Unplanned interruption of services leading to an inability to trade Kyoto Protocol emissions and fulfil compliance obligations;

(c) The violation of internal or external regulations resulting in judicial proceedings, penalties or disciplinary measures;

(d) Damage to the reputation of emissions trading mechanisms in general terms.

18. Based on the international standard ISO/IEC 27002,[9] the SWG prepared a control baseline that includes 95 technical, administrative and physical controls. These controls prevent, detect, correct and deter illegitimate access and uncontrolled modification of the emissions trading IT systems and assist in removing environmental influences that limit registry operations.

E. Security Working Group evaluation of controls

1. Control implementation guidance

19. Subsequent to the initial risk review and guidance provided by ISO/IEC 27001 and DES, the SWG applied implementation guidance to the 95 controls included in the baseline. The SWG categorizes these controls as:

(a) **Mandatory** when required by DES (subtotal: 27);

[9] ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls.

(b) **Normative** when assumed obligatory by ISO/IEC 27001 to be selected as a part of an ISMS planning and implementation process (subtotal: 50);

(c) **Recommended** when not assumed obligatory by ISO/IEC 27001 or DES, but supporting controls with normative or mandatory implementation guidance (subtotal: 18).

20. Furthermore, the SWG associated all the controls included in the baseline with a qualitative cost estimate. The level of cost related to implementing each control is estimated as:

(a) **High** for controls that require procuring, implementing and operating systems that currently do not exist within the architecture or organization of emissions trading systems;

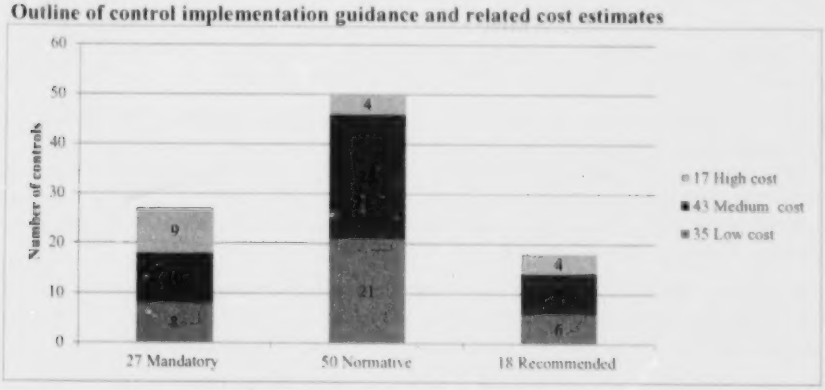
(b) **Medium** for controls that require implementing and operating additional features to systems that currently do exist within the architecture or organization of emissions trading systems;

(c) **Low** for controls that currently do exist within the architecture or organization of emissions trading systems or for controls that entail low expenditures in operation and procurement efforts.

21. An outline of control implementation guidance and related cost estimates is represented in figure 1.

Figure 1

Outline of control implementation guidance and related cost estimates



2. Control implementation survey

22. To support the SWG in evaluating the existing controls and identifying options to promote or improve security management, an initial survey was sent to all RSAs to conduct an assessment of the implementation status of the required technology and processes.

23. Subsequently, 17 national registries voluntarily responded to the initial survey. The response included 13 submissions from the Consolidated System of European Union Registries (CSEUR) and four submissions from non-CSEUR registries. As originally anticipated, the survey results confirmed that mandatory controls have already been implemented and that normative and recommended controls have been partially implemented. In addition, the survey reiterated that the consistent application of controls in systems supporting emissions trading under the Kyoto Protocol is not currently guaranteed.

III. Options identified by Security Working Group

24. Based on the control baseline and the initial implementation survey, the SWG identified two options to facilitate ISMS implementation in systems supporting emissions trading under the Kyoto Protocol. These options are **business as usual** and **further implementation**, which are outlined below.

A. Option 1: business as usual

25. The business as usual option refers to a normal execution of standard information security operations within systems supporting emissions trading under the Kyoto Protocol. These operations are already defined in the existing DES and are mandatory for all registry systems connected to the ITL.

26. DES includes controls related to authentication and authorization; test, change and release management; information handling and exchange; system monitoring and logging; and transaction validation. In contrast, DES does not include controls related to asset management, information security roles and responsibilities, physical and environmental security, and information security incident management.

27. The business as usual option addresses only the current situation and does not mandate additional activities to improve information security. Consequently, this option does not introduce additional efforts or costs because, within it, no new guidance would be defined. Selecting the business as usual option confirms the role and responsibilities of individual national registries to implement security controls in the absence of additional guidance.

28. Selecting the business as usual option implies the acceptance of the risk of misinterpreting security incidents due to the fact that relevant assets would not be properly classified. Moreover, security incidents would go unrecognized owing to absent reporting structures. This option also implies acceptance of the risk of environmental events that limit or cease the ability of sites to support the emissions trading systems owing to an inadequate implementation of physical controls.

29. As the business as usual option implies the acceptance of the above-mentioned risks and does not improve consistency in the application of security controls in systems supporting emissions trading under the Kyoto Protocol, it is not recommended.

B. Option 2: further implementation

30. The further implementation option refers to a structured and planned extension of the current information security control implementation in systems supporting emissions trading under the Kyoto Protocol. The further implementation option requires an additional registry-specific and quantitative risk assessment, followed by an in-depth control implementation analysis. Based on further evaluation of the control implementation, improvement options will be identified. The additional controls selected for implementation will be prioritized based on the control's risk mitigation capabilities and risk probabilities.

31. Selecting the further implementation option will consequently result in additional efforts and costs related to:

(a) National registries and the ITL administrator implementing secure data exchange methods and procedures;

(b) National registries conducting additional risk assessments by applying recognized methodologies;

(c) The SWG nominating and prioritizing control implementations;

(d) The SWG defining criteria to monitor the implementation progress and the effectiveness of controls;

(e) National registries systematically implementing the selected controls in registry operations;

(f) National registries reporting on the status of control implementation;

(g) The SWG systematically monitoring the status of control implementation.

32. Based on the further implementation option, the SWG identified a need to strengthen its capacity by engaging an external expert with information security specific skills. This security expert would be responsible for identifying methods to support risk assessments; planning, preparing and executing applicable control implementations; and supporting the operation of ISMS.

IV. Implementation road map

33. Further steps for implementing additional security controls in systems supporting emissions trading under the Kyoto Protocol are projected in the road map (figure 2). Each step in the road map includes key performance indicators (KPIs) to measure the progress and effectiveness of ISMS implementation.

34. Steps 1–4 of the road map refer to the preparation phase of ISMS implementation. This phase includes the definition of ISMS scope; a qualitative exploration of known threats, vulnerabilities and consequences; and the preliminary definition of a control baseline. The preparation phase has been completed by developing this document.

35. Steps 5–8 of the road map refer to the planning phase of ISMS implementation. Based on further guidance from the SBI at its fortieth session, the process will either be completed by selecting the business as usual option or will commence, should the further implementation option be selected, with a detailed, registry-specific and quantitative risk assessment, followed by an in-depth control implementation analysis. A subsequent implementation status gap analysis would provide an input to the prioritization and detailed planning of additional control implementation. The planning phase would be concluded by the SBI considering and providing further guidance on the preferred implementation option. The selected option would define additional steps, which will be completed during the execution phase.

36. Step 9 of the road map refers to the execution of the selected implementation option.

37. Steps 10–12 refer to the operation of ISMS. Controls implemented during the execution phase must be monitored to effectively recognize and respond to information security incidents and to continuously improve ISMS.

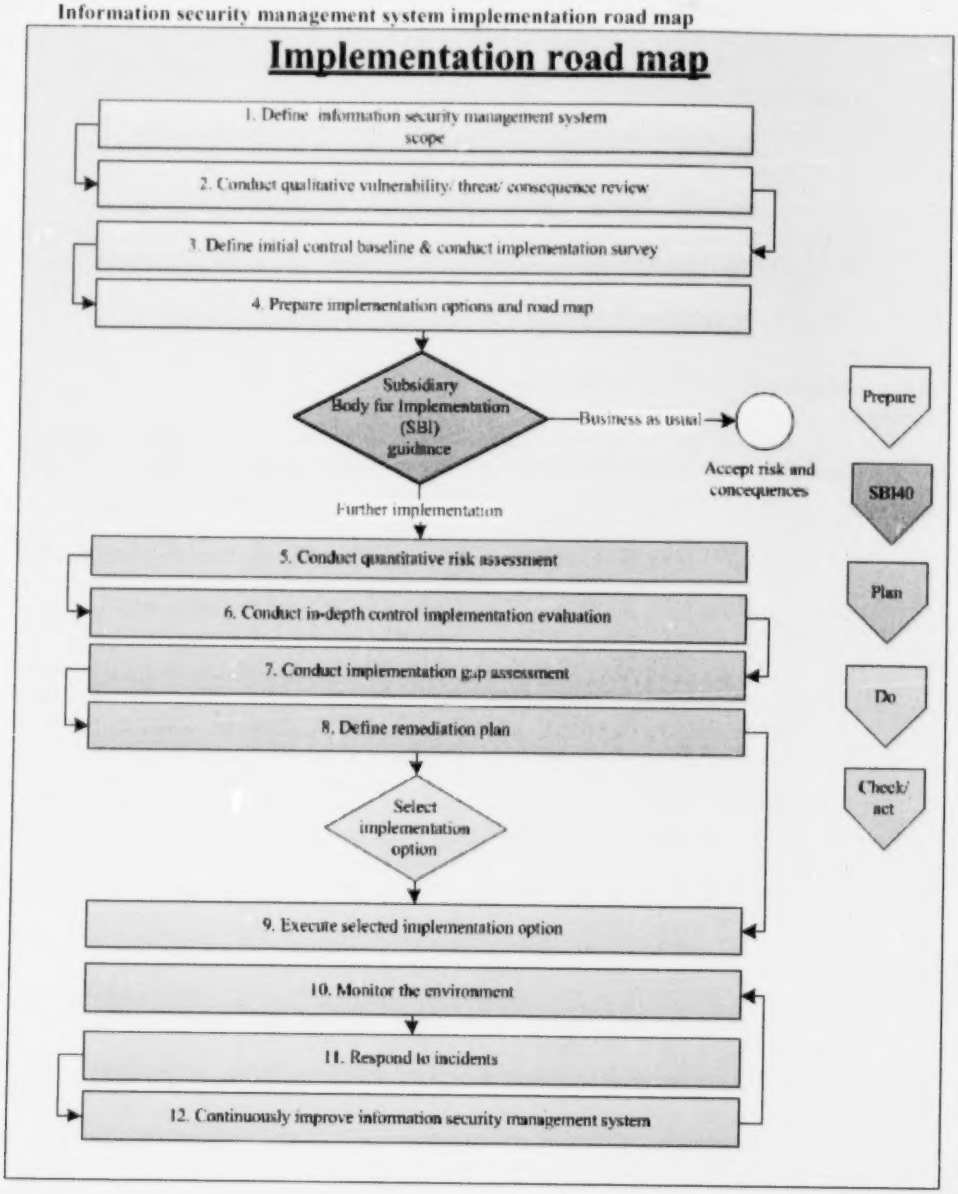
38. The planning phase has been initiated by preparing the ISMS implementation options and road map included in this document. Should the SBI at its fortieth session decide to proceed with the further implementation option, the planning activities included in steps 5–8 will be completed in order to define and recommend the final implementation option.

39. Information on the progress of the work conducted by the SWG would be provided to the SBI through the annual reports of the ITL administrator, with a view to providing

guidance, as necessary, in relation to a structured and planned extension of the current information security control implementation in systems supporting emissions trading under the Kyoto Protocol.

Figure 2

Information security management system implementation road map


Implementation road map
1. Define information security management system scope
2. Conduct qualitative vulnerability/ threat/ consequence review
3. Define initial control baseline & conduct implementation survey
4. Prepare implementation options and road map
Subsidiary Body for Implementation (SBI) guidance
Business as usual
Accept risk and concequences
Further implementation
5. Conduct quantitative risk assessment
6. Conduct in-depth control implementation evaluation
7. Conduct implementation gap assessment
8. Define remediation plan
Select implementation option
9. Execute selected implementation option
10. Monitor the environment
11. Respond to incidents
12. Continuously improve information security management system
Prepare
SBI40
Plan
Do
Check/ act

V. Monitoring and continuous improvement

40. Should the SBI at its fortieth session decide to proceed with the further implementation option, the upcoming activities would include methods to monitor and measure progress towards achieving the planned milestones and improving security awareness.

41. Progress and costs would be monitored on an on-going basis to determine conformance with the implementation plan and to allow for mid-course corrections on a timely basis. The measuring of implementation progress will benefit from developing an appropriate set of KPIs.

42. KPIs indicating a successful ISMS implementation could include:

(a) Quantitative identification, categorization and definition of risks and risk mitigating controls;

(b) Definition and execution of appropriate tests to confirm the effectiveness and compliance of implemented controls;

(c) Progress in control implementation and effectiveness testing;

(d) Resources committed to accomplishing the risk assessment, executing the control implementation and to reporting on the implementation progress.

43. Compliance reporting and monitoring based on KPIs can follow existing reporting processes. Decision 15/CMP.1, annex, paragraph 22, requires Annex I Parties to provide in national inventory reports (NIRs) information on any changes that have occurred in the national registries. This includes information submitted in accordance with decision 15/CMP.1, annex, paragraph 32(f), which requires each Annex I Party to provide a description of how security measures are employed in the national registry and how these measures are kept up to date.

44. To enable compliance reporting and monitoring, additional guidance on specific security reporting requirements and inclusion of classified information in NIRs and SIARs is to be provided by the CMP.

45. Combined with the selection of the ISMS implementation option, it is expected that the SBI will be requested to consider additional technical and administrative roles required to effectively operate ISMS. Roles in accordance with the specific implementation guidance include information security specialists, architects and programme managers. Finally, it must be ensured that personnel in the security-related roles maintain the appropriate skills needed to carry out activities supporting the existing information systems and the implemented information security controls.

Annex

Glossary

Annex I Party	Party included in Annex I to the Convention
Asset	Any item that is valuable to the systems supporting emissions trading under the Kyoto Protocol, including information, software, hardware, services, people and intangibles, such as reputation and public perception
Availability	Property of being accessible and usable upon demand by an authorized entity
Control	Means of managing risk, including policies, procedures, guidelines, practices and organizational structures, which can be administrative, logical (technical) or administrative in nature
Confidentiality	Property of being available or disclosed to authorized individuals, entities or processes only
Emissions trading	System of interconnected databases and applications, including the international transaction log (ITL), national registries connected to the ITL, the clean development mechanism registry, the compilation and accounting database, the Consolidated System of European Union Registries and the interconnecting data communication
Information security	Preservation of the confidentiality, integrity and availability of information
Information security management system	Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
Information security incident	Occurrence or change of a particular set of circumstances with one or more occurrences and various possible causes, referred to in this document as an "incident"
Information security risk	Effect of uncertainty on objectives expressed in terms of a combination of the consequences of an information security incident and the associated likelihood of occurrence
Integrity	Property of protecting the accuracy and completeness of assets
National registry	An electronic database maintained by a Party or a group of Parties for the transfer and tracking of units in accordance with the Kyoto Protocol rules

Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk analysis	Process to comprehend the nature of risk and to determine the risk level
Risk criteria	Terms of reference against which the significance of risk is evaluated
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable
Risk identification	Process of finding, recognizing and describing risks
Risk level	Magnitude of a risk expressed as "low", "medium" or "high", combining consequences and their likelihood
System	Software application, service, information technology asset or any other information handling component
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats